IN THE CLAIMS:

1. (Previously presented) A service provider system for implementing changes in the security of a plurality of customer systems with a first subsystem (1) that does not have data as to the system characteristics of individual customer systems, comprising: means for providing activation tokens (6, 7, 8) to be transmitted to at least two customers with a second subsystem (2) for receiving said activation tokens, said means for providing activation tokens (6, 7, 8) including means for providing activation information (7) and means for naming of system characteristics of a plurality of second subsystems in machine readable and filterable manner (6), wherein the relevance of said activation information to said second subsystem (2) can be determined by said second subsystems checking whether said second subsystem (2) has characteristics corresponding to said naming of said activation token, so that receipt by a customer system of an activation token does not indicate whether that token is relevant to the second subsystem of that customer.

2. (previously presented) Service provider system as claimed in claim 1, wherein said means for providing activation tokens (6, 7, 8) include cryptographic means (8) for encrypting the activation tokens and signing means for producing a verification information to be verified by said second subsystem (2) of said customer.

3. (previously presented) A customer system with a second subsystem (2) for receiving activation tokens, including both tokens relevant to said customer system and tokens not relevant to said customer system, provided by a service provider with a first subsystem that does not have data as to the system characteristics of individual customer systems, for implementing changes in the security of said customer system (1), said activation tokens including activation information and naming of system characteristics in machine readable and filterable manner, said second subsystem (2) comprising:

receiving means (11) for controlling said receiving of said activation tokens,
checking means (12) for automatically determining whether said activation information is relevant for said second subsystem (2) by checking whether said second subsystem (2) has characteristics

corresponding to said naming of an activation token, and transforming means (13) for transforming relevant activation information into at least one activation measure for said second subsystem (2) that implements a change in the security of said customer system.

4. (previously presented) Customer system as claimed in claim 3, wherein said receiving means (11) include cryptographic means for verifying said service provider as being the provider of said activation token and admitting means for controlling whether said service provider is legitimated to send activation tokens to said customer.

5. (original) Customer system as claimed in claim 3, wherein said transforming means (13) include at least one set of filter parameters to enable transforming of said relevant activation information into at least one acceptable activation measure.

6. (previously presented) Customer system as claimed in claim 3, wherein said second subsystem (2) includes implementation means (14) for automatically implementing at least one activation measure and reporting implemented activation measures.

7. (canceled)

8. (canceled)

9. (previously presented) Customer system as claimed in claim 3, wherein said receiving means (11), checking means (12) and transforming means (13) of said second subsystem (2) are part of an apoptosis system realized by at least one means out of the group of a daemon, a kernel module, an initab, an inetd, tcp-wrapper, a rpcbind, a resource manager, a network management, and a hardware device.

10. (previously presented) A system for supplying activation information to a subsystem, said system comprising:
a service provider with a first subsystem (1) that does not have data as to the system characteristics of individual customer systems, for providing activation tokens for implementing changes in the security of a plurality of customer systems to at least two customers with a second subsystem (2) for receiving said activation tokens including both tokens relevant to said customer system and tokens not relevant to said customer system, said activation tokens including activation information and naming of system

characteristics of a plurality of second subsystems in machine readable and filterable manner, wherein said second subsystem (2) comprises receiving means (11) for controlling said receiving of said activation tokens, checking means (12) for automatically determining whether said activation information is relevant for said second subsystem (2) by said second subsystem checking whether said second subsystem (2) has characteristics corresponding to said naming of an activation token, so that receipt by a customer system of an activation token does not indicate whether that token is relevant to the second subsystem of that customer, and transforming means (13) for transforming relevant activation information into at least one activation measure for said second subsystem (2).

11. (previously presented) System as claimed in claim 10, wherein said receiving means (11) include cryptographic means for verifying said service provider as being the provider of said activation token, and wherein said receiving means (11) include admitting means for controlling whether said service provider is legitimated to send activation tokens to said customer.

12. (original) System as claimed in claim 10, wherein said transforming means (13) include at least one set of filter parameters to enable transforming of said relevant activation information into at least one acceptable activation measure.

13. (original) System as claimed in claim 10, wherein said second subsystem (2) includes implementation means (14) for implementing at least one activation measure.

14. (original) System as claimed in claim 13, wherein said implementation means (14) include at least ane reporting means for reporting implemented activation measures.

15. (original) System as claimed in claim 10, wherein said naming includes the specification of a version, platform and a configuration corresponding to said second subsystem (2).

16 . (previously presented) System as claimed in claim 10, wherein said receiving means (11), checking means (12) and transforming (13) means of said second subsystem (2) are part of an apoptosis system realized by at least one means out of the group of a daemon, a kernel module, an inittabo an inetd, tcp-

wrapper, a rpcbind, a resource manager, a network management, and a hardware device.

17. (original) System as claimed in claim 13, wherein said system is reducing the vulnerability of said second subsystem (2) by automatically implementing activation measures at said second subsystem(2).

18. (original) A method for providing activation information by a service provider with a first subsystem (1) to a customer with a second subsystem (2) comprising the step of:
providing activation tokens by said service provider, wherein said activation tokens include readable activation information and naming of corresponding system characteristics in machine readable and filterable manner.

19. (Canceled)

20. (Canceled)

21. (previously presented) A method for using activation information for implementing changes in the security of a plurality of

customer systems by a customer with a second subsystem (2), said activation information being provided by service provider with a first subsystem (1) that does not have data as to the system characteristics of individual customer systems, to at least two customers in the form of activation tokens including said activation information and naming of corresponding system characteristics of a plurality of second subsystems in machine readable and filterable manner, said method comprising the steps of:

receiving both relevant and non-relevant activation tokens by said second subsystem (2), automatically determining whether said activation information is relevant for the second subsystem (2) by automatically checking by said second subsystem (2) whether said second subsystem (2) has characteristics corresponding to said naming of an activation token, so that receipt by a customer system of an activation token does not indicate whether that token is relevant to the second subsystem of that customer and transforming relevant activation information into at least one activation measure for said second subsystem(2).

22. (previously presented) Method as claimed in claim 21, further comprising the step of verifying at said second subsystem (2)

whether said service provider is legitimated to send activation tokens to said customer.

23. (original) Method as claimed in claim 21, wherein said transforming includes filtering of said activation information by at least one set of filter parameters to get at least one acceptable activation measure.

24. (previously presented) Method as claimed in claim 21, further comprising the step(s) of implementing at least one activation measure and reporting implemented activation measures.

25. (previously presented) Method as claimed in claim 21, wherein said checking by said second subsystem (2) includes checking whether said second subsystem (2) has a version, platform or configuration corresponding to said naming of an activation token.

26. (original) Method as claimed in claim 21, further comprising a step of automatically implementing at least one activation measure to said second subsystem (2).

27. (previously presented) Method as claimed in claim 26, further comprising the step of automatically implementing at least one activation measure leads to a reduction of vulnerability of said second subsystem (2) and enables a shutdown of a service of said second subsystem (2).

28. (currently amended) A computer program comprising program code means for performing the method of claim 21 when said program is run on a computer.

29. (previously presented) A computer program product comprising program code means stored on a computer readable medium for performing the method of claim 21 when said program is run on a computer.